property under DoD jurisdiction is sexually explicit, such material shall be withdrawn from all retail outlets where it is sold or rented and returned to distributors or suppliers, and shall not be purchased absent further action by the Board.

(c) The Board shall convene as necessary to determine whether any material offered or to be offered for sale or rental on property under DoD jurisdiction is sexually explicit. The Board members shall, to the extent practicable, maintain and update relevant information about material offered or to be offered for sale or rental on property under DoD jurisdiction.

(d) If any purchasing agent or manager of a retail outlet has reason to believe that material offered or to be offered for sale or rental on property under DoD jurisdiction may be sexually explicit as defined herein, and such material is not addressed by the Board's guidance issued pursuant to paragraph (e) of this section, he or she shall request a determination from the Board about such material prior to purchase or as soon as possible.

(e) At the conclusion of each review and, as necessary, the Board shall issue guidance to purchasing agents and managers of retail outlets about the purchase, withdrawal, and return of sexually explicit material. The Board may also provide guidance to purchasing agents and managers of retail outlets about material that it has determined is not sexually explicit. Purchasing agents and managers of retail outlets shall continue to follow their usual purchasing and stocking practices unless instructed otherwise by the Board.

(f) Material which has been determined by the Board to be sexually explicit may be submitted for reconsideration every 5 years. If substantive changes in the publication standards occur earlier, the purchasing agent or manager of a retail outlet under DoD jurisdiction may request a review.

§ 235.7 Information requirements.

The Chair of the Board shall submit to the PDUSD(P&R) an annual report documenting the activities, decisions, and membership of the Board. Negative reports are required. The annual report shall be due on October 1st of each year and is not subject to the licensing internal information requirements of DoD 8910.1–M.[2]

PART 236—DEPARTMENT OF DEFENSE (DoD)—DEFENSE INDUSTRIAL BASE (DIB) CYBER SECURITY (CS) ACTIVITIES

Sec.

AUTHORITY: 10 U.S.C. 391; 10 U.S.C. 2224; 44 U.S.C. 3506; 44 U.S.C. 3544; and Section 941, Publ. L. 112–239, 126 Stat. 1632.

SOURCE: 80 FR 59584, Oct. 2, 2015, unless otherwise noted.

§ 236.1 Purpose.

Cyber threats to contractor unclassified information systems represent an unacceptable risk of compromise of DoD information and pose an imminent threat to U.S. national security and economic security interests. This part requires all DoD contractors to rapidly report cyber incidents involving covered defense information on their covered contractor information systems or cyber incidents affecting the contractor's ability to provide operationally critical support. The part also modifies the eligibility criteria to permit greater participation in the voluntary DoD–DIB CS information sharing program in which DoD provides cyber threat information and cybersecurity best practices to DIB participants. The DoD–DIB CS information sharing program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

§ 236.2 Definitions.

As used in this part:

[2] Copies may be obtained at *http://www.dtic.mil/whs/directives/*.

Access to media means provision of media, or access to media physically or remotely to DoD personnel, as determined by the contractor.

Cleared defense contractor (CDC) means a private entity granted clearance by DoD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of DoD.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Contractor means an individual or organization outside the U.S. Government who has accepted any type of agreement or order to provide research, supplies, or services to DoD, including prime contractors and subcontractors.

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (*e.g.*, program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, ''Distribution Statements of Technical Documents,'' available at *http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf*. The term does not include information that is lawfully publicly available without restrictions.

Covered contractor information system means an information system that is owned or operated by or for a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified information that:

(1) Is:

(i) Provided to the contractor by or on behalf of the DoD in connection with the performance of a contract; or

(ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of a contract; and

(2) Falls in any of the following categories:

(i) Controlled Technical Information;

(ii) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process);

(iii) Export Control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information;

(iv) Any other information, marked or otherwise identified by the Government, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (*e.g.*, privacy, proprietary business information).

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Cyber incident damage assessment means a managed, coordinated process to determine the effect on defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from compromise of a

contractor's unclassified computer system or network.

Defense Industrial Base (DIB) means the Department of Defense, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements.

DIB participant means a CDC that has met all of the eligibility requirements to participate in the voluntary DoD–DIB CS Information Sharing Program as set forth in this part (see § 236.7).

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Government furnished information (GFI) means information provided by the Government under the voluntary DoD–DIB CS information sharing program including but not limited to cyber threat information and cybersecurity practices.

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Malicious software means software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Media means physical devices or writing surfaces, including but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered Contractor information system.

Operationally critical support means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

Rapid(ly) report(ing) means within 72 hours of discovery of any cyber incident.

Technical Information means technical data or computer software, as those terms are defined in DFARS 252.227–7013, ''Rights in Technical Data—Noncommercial Items'' (48 CFR 252.227–7013). Examples of technical information include research and engineering data, engineering drawings and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Threat means any circumstance or event with the potential to adversely impact organization operations (including mission, functions, image, or reputation), organization assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

U.S. based means provisioned, maintained, or operated within the physical boundaries of the United States.

U.S. citizen means a person born in the United States or naturalized.

§ 236.3 Policy.

It is DoD policy to:

(a) Establish a comprehensive approach to require safeguarding of covered defense information on covered contractor information systems and to require contractor cyber incident reporting.

(b) Increase Government stakeholder and DIB situational awareness of the extent and severity of cyber threats to DoD information by implementing a streamlined approval process that enables the contractor to elect, in conjunction with the cyber incident reporting and sharing, the extent to